Electronic Colloquium on Computational Complexity, Report No. 193 (2016)

Identity Testing for +-Regular Noncommutative Arithmetic Circuits

V. Arvind* Pushkar S Joglekar† Partha Mukhopadhyay‡ S. Raja§

November 22, 2016

Abstract

An efficient randomized polynomial identity test for noncommutative polynomials given by noncommutative arithmetic circuits remains an open problem. The main bottleneck to applying known techniques is that a noncommutative circuit of size s can compute a polynomial of degree exponential in s with a double-exponential number of nonzero monomials. In this paper, which is a follow-up on our earlier article [AMR16], we report some progress by dealing with two natural subcases (both allow for polynomials of exponential degree and a double exponential number of monomials):

1. We consider *+-regular* noncommutative circuits: these are homogeneous noncommutative circuits with the additional property that all the +-gates are layered, and in each +-layer all gates have the same syntactic degree. We give a *white-box* polynomial-time deterministic polynomial identity test for such circuits. Our algorithm combines some new structural results for +-regular circuits with known results for noncommutative ABP identity testing [RS05], rank bound of commutative depth three identities [SS13], and equivalence testing problem for words [Loh15, MSU97, Pla94].
2. Next, we consider $\Sigma\Pi^*\Sigma$ noncommutative circuits: these are noncommutative circuits with layered +-gates such that there are only two layers of +-gates. These +-layers are the output +-gate and linear forms at the bottom layer; between the +-layers the circuit could have any number of $\times$ gates. We given an efficient randomized *black-box* identity testing problem for $\Sigma\Pi^*\Sigma$ circuits. In particular, we show if $f \in \mathbb{F}\langle Z\rangle$ is a nonzero noncommutative polynomial computed by a $\Sigma\Pi^*\Sigma$ circuit of size s, then f cannot be a polynomial identity for the matrix algebra $\mathbb{M}_s(F)$, where the field F is a sufficiently large extension of $\mathbb{F}$ depending on the degree of f.

1 Introduction

Noncommutative arithmetic computation is an important area of algebraic complexity theory, introduced by Hyafil [Hya77] and Nisan [Nis91]. The main algebraic structure of interest is the free noncommutative ring $\mathbb{F}\langle Z\rangle$ over a field $\mathbb{F}$, where $Z = \{z_1, z_2, \cdots, z_n\}$ is a set of n free noncommuting variables. The elements of $\mathbb{F}\langle Z\rangle$ are *noncommutative polynomials* which are $\mathbb{F}$-linear combinations of *monomials*, which, in turn, are words in Z^*.

*Institute of Mathematical Sciences (HBNI), Chennai, India, `email: arvind@imsc.res.in`
†Vishwakarma Institute of Technology, Pune, India, `email: joglekar.pushkar@gmail.com`
‡Chennai Mathematical Institute, Chennai, India, `email: partham@cmi.ac.in`
§Chennai Mathematical Institute, Chennai, India, `email: sraja@cmi.ac.in`

ISSN 1433-8092

An important algorithmic problem in this area is noncommutative polynomial identity testing: The input is a noncommutative polynomial $f \in \mathbb{F}\langle Z\rangle$ computed by a noncommutative arithmetic circuit C. The polynomial f can be either given by black-box access to C (using which we can evaluate C on matrices with entries from $\mathbb{F}$ or an extension field), or the circuit C may be explicitly given as the input. The algorithmic problem is to check if the polynomial computed by C is identically zero.

We recall the formal definition of a noncommutative arithmetic circuit.

Definition 1. *A* noncommutative arithmetic circuit C *over a field* $\mathbb{F}$ *and indeterminates* $z_1, z_2, \cdots, z_n$ *is a directed acyclic graph (DAG) with each node of indegree zero labeled by a variable or a scalar constant from* $\mathbb{F}$*: the indegree* 0 *nodes are the input nodes of the circuit. Each internal node of the DAG is of indegree two and is labeled by either a* $+$ *or a* $\times$ *(indicating that it is a plus gate or multiply gate, respectively). Furthermore, the two inputs to each* $\times$ *gate are designated as left and right inputs which is the order in which the gate multiplication is done. A gate of* C *is designated as* output*. Each internal gate computes a polynomial (by adding or multiplying its input polynomials), where the polynomial computed at an input node is just its label. The* polynomial computed *by the circuit is the polynomial computed at its output gate. An arithmetic circuit is a formula if the fan-out of every gate is at most one.*

Notice that if the size of circuit C is s the degree of the polynomial computed by C can be 2^s. In the earlier result [1] by Bogdanov and Wee [BW05], a randomized polynomial-time algorithm was shown for the case when the degree of the circuit C is polynomially bounded in s and n [BW05]. The idea of the algorithm is based on a classical result of Amitsur-Levitzki [AL50]. We recall the Amitsur-Levitzki theorem.

Theorem 1 (Amitsur-Levitzki Theorem)**.** *For any field* $\mathbb{F}$*, a nonzero noncommutative polynomial* $P \in \mathbb{F}\langle Z\rangle$ *of degree* $\leq 2d-1$ *cannot be a polynomial identity for the matrix algebra* $\mathbb{M}_d(\mathbb{F})$*. I.e.* P *does not vanish on all* $d \times d$ *matrices over* $\mathbb{F}$*.*

Bogdanov and Wee's randomized PIT algorithm [BW05] applies the above theorem to obtain a randomized PIT as follows: Let $C(z_1, z_2, \cdots, z_n)$ be a circuit of syntactic degree bounded by $2d-1$. For each $i \in [n]$, substitute the variable z_i by a $d \times d$ matrix M_i of commuting indeterminates. More precisely, the $(\ell, k)^{th}$ entry of M_i is $z_{\ell,k}^{(i)}$ where $1 \leq \ell, k \leq d$. By Theorem 1, the matrix $M_f = f(M_1, M_2, \ldots, M_n)$ is not identically zero. Hence, in M_f there is an entry (ℓ', k') which has the *commutative* nonzero polynomial $g_{\ell',k'}$ over the variables $\{z_{\ell,k}^{(i)} : 1 \leq i \leq n, 1 \leq \ell, k \leq d\}$. Notice that the degree of the polynomial $g_{\ell',k'}$ is at most $2d-1$. If we choose an extension field of $\mathbb{F}$ of size at least $4d$, then we get a randomized polynomial identity testing algorithm by the standard Schwartz-Zippel-Lipton-DeMello Lemma [Sch80, Zip79, DL78].

The problem with this approach for general noncommutative circuits (whose degree can be 2^s) is that the dimension of the matrices grows linearly with the degree of the polynomial. Therefore, this approach only yields a randomized exponential-time algorithm for the problem. Finding an efficient randomized identity test for general noncommutative circuits is a well-known open problem, as mentioned in a recent workshop on algebraic complexity theory [WACT16].

[1] We also note here that Raz and Shpilka [RS05] give a white-box deterministic polynomial-time identity test for noncommutative algebraic branching programs (ABPs). The results of Forbes-Shpilka [FS13] and Agrawal et al., [AGKS15] give (among other results) a quasi-polynomial time black-box algorithm for small degree noncommutative ABPs.

In [AMR16], we made partial progress on this problem: we gave an efficient randomized black-box polynomial identity test for noncommutative arithmetic circuits that compute a polynomial with *exponentially many* monomials [AMR16]. However, in general noncommutative circuits of size $O(s)$ can compute polynomials with 2^{2^s} monomials. For example the polynomial $f(x, y) = (x+y)^{2^s}$ has noncommutative circuit of size $O(s)$ but the number of monomials is 2^{2^s}.

2 Main Results

We first consider identity testing for a subclass of homogeneous noncommutative circuits, that we call $+$-regular circuits. These are syntactic homogeneous circuits where the $+$-gates can be partitioned into layers such that: (i) there is no directed paths between the $+$-gates in a same layer, and (ii) all $+$-gates in a layer have the same syntactic degree. The output gate is a $+$ gate. We give a deterministic white box polynomial-time algorithm that tests whether a given noncommutative $+$-regular circuit of size s computes the identically zero polynomial.

Theorem 2. *Let C be a noncommutative $+$-regular circuit of size s given as a white-box computing a polynomial in $\mathbb{F}\langle X\rangle$. There is a deterministic polynomial-time algorithm that tests whether C computes the identically zero polynomial.*

Next, we consider $\Sigma\Pi^*\Sigma$ noncommutative circuits. These are noncommutative circuits with layered $+$-gates such that there are only two layers of $+$-gates. These $+$-layers are the output $+$-gate and linear forms at the bottom layer; between the $+$-layers the circuit could have any number of $\times$ gates. We give an efficient randomized black-box polynomial identity test for $\Sigma\Pi^*\Sigma$ circuits. More precisely, we show the following result.

Theorem 3. *Let $\mathbb{F}$ be a field of size more than D. Let $f(x_1, \ldots, x_n) \in \mathbb{F}\langle X\rangle$ be a nonzero polynomial of degree D computed by a homogeneous $\Sigma\Pi^*\Sigma$ circuit with top gate fan-in s and the fan-in of the product gates bounded by D. Then f cannot be a polynomial identity for the matrix algebra $\mathbb{M}_s(\mathbb{F})$.*

Corollary 1. *Let C be a homogeneous $\Sigma\Pi^*\Sigma$ circuit of size s computing a polynomial $f(x_1, \ldots, x_n) \in \mathbb{F}\langle X\rangle$, where C is given by black-box access. There is a randomized* $\mathrm{poly}(s, n)$ *time algorithm that checks whether f is identically zero.*

Outline of the proofs

We give an informal outline of the proofs for Theorem 2, and Theorem 3.

White-box algorithm for +-regular circuits

Now we informally describe the proof of Theorem 2. We note a crucial observation: Let $T(z_1, \ldots, z_s)$ be a homogeneous noncommutative polynomial of degree d. Let $R_1, \ldots, R_s$ be homogeneous noncommutative polynomials each of degree d'. Consider any maximal $\mathbb{F}$-linearly independent subset of the polynomials $R_1, \ldots, R_s$. Let $R_1, \ldots, R_k$ be such a set. We can express $R_j = \sum_{i=1}^{k} \alpha_{ji} R_i$ for $k+1 \le j \le s$ where $\alpha_{ji} \in \mathbb{F}$. Then it turns out that $T(R_1, \ldots, R_k, \sum_{i=1}^{k} \alpha_{k+1i} R_i, \ldots, \sum_{i=1}^{k} \alpha_{si} R_i) = 0$ if and only if $T(y_1, \ldots, y_k, \sum_{i=1}^{k} \alpha_{k+1i} y_i, \ldots, \sum_{i=1}^{k} \alpha_{si} y_i) = 0$ where $y_1, \ldots, y_k$ are fresh noncommuting variables. As a consequence, it turns out that for a deterministic polynomial-time white-box identity testing for $+$-regular circuits, it suffices to solve the following computational problem:

Let $P_1, \ldots, P_\ell \in \mathbb{F}\langle X\rangle$ be products of homogeneous linear forms given by *multiplicative circuits* of size s. The degrees of the polynomials P_i could be exponential in s. Then find a maximal $\mathbb{F}$-linearly independent subset of the polynomials and express the others as linear combination of the independent polynomials. We solve the above problem in deterministic polynomial time. We prove that it suffices to replace P_i with $\tilde{P}_i$ which is obtained from P_i by retaining, in the product, only linear forms that appear in at most ℓ^5 locations (roughly). This is shown using a rank bound result of commutative depth three identities [SS13]. We also require algorithms [Loh15, Pla94, MSU97] over words to efficiently find the linear forms appearing in those ℓ^5 locations. Since $\tilde{P}_i : 1 \leq i \leq \ell$ are small degree, we are in the usual regime of low-degree noncommutative polynomials, and can adapt the noncommutative ABP identity testing [RS05] to solve the linear independence testing problem.

Black-box algorithm for homogeneous $\Sigma\Pi^*\Sigma$ circuits

Now, we briefly sketch the proof of Theorem 3. Suppose $P_1, P_2, \ldots, P_s$ are D-products of homogeneous linear forms in $\mathbb{F}\langle X\rangle$. Consider any $\mathbb{F}$-linear combination $\sum_{i=1}^{s} \beta_i P_i$ where, w.l.o.g $\forall i : \beta_i \in \mathbb{F} \setminus \{0\}$. Then there is a subset of indices $I \subseteq [D]$ with $|I| \leq s-1$ with the following property: For each i, let $P_{i,I}$ be the polynomial obtained from P_i by treating only the variables appearing in positions in I as noncommutative, and variables in all other positions as commutative. Then

$$\sum_{i=1}^{s} \beta_i P_i = 0 \text{ iff } \sum_{i=1}^{s} \beta_i P_{i,I} = 0.$$

Now, we can design small nondeterministic substitution automata that can nondeterministically effect this transformation from P_i to $P_{i,I}$ for each i. guess the locations in I. The rest of the proof is similar to the proof of Theorem 2 in [AMR16].

3 Preliminaries

We state some useful properties of noncommutative polynomials.

Proposition 1. *Let $A : \mathbb{F}^n \to \mathbb{F}^n$ be any invertible linear transformation, and $f(x_1, x_2, \ldots, x_n) \in \mathbb{F}\langle X\rangle$ be any homogeneous polynomial of degree d. Let $A_j(f)$ be the polynomial obtained by replacing the variables x_i appearing in the position $j \in [d]$ by $A(x_i)$. Then $f(x_1, \ldots, x_n) \neq 0$ if and only if $A_j f(x_1, \ldots, x_n) \neq 0$.*

Proof. If $f(x_1, \ldots, x_n) = 0$ then clearly $A_j f(x_1, \ldots, x_n) = 0$. Suppose $f(x_1, \ldots, x_n) \neq 0$. Write $f = \sum_{(m_1,m_2)} f_{m_1,m_2}$, where

$$f_{m_1,m_2} = m_1 \ L_{m_1,m_2} \ m_2,$$

and (m_1, m_2) runs over monomial pairs such that m_1 is of degree $j-1$ and m_2 is of degree $d-j$. Here, L_{m_1,m_2} denotes the linear form in the variables $x_1, x_2, \ldots, x_n$ occurring in j^{th} position when we collect together all monomials of the form $m_1 x_i m_2$, $1 \leq i \leq n$. Notice that

$$A_j(f) = \sum_{m_1,m_2} A_j(f_{m_1,m_2}) = \sum_{m_1,m_2} m_1 A(L_{m_1,m_2}) m_2.$$

Since $f \neq 0$, for some pair (m_1, m_2) we have $f_{m_1,m_2} \neq 0$. In particular, $L_{m_1,m_2} \neq 0$. Since A is invertible, it follow that $m_1 A(L_{m_1,m_2}) m_2 \neq 0$. Therefore, $A_j(f) \neq 0$. □

Given any noncommutative polynomial $f(x_1, \ldots, x_n) \in \mathbb{F}\langle X \rangle$ of degree d, we can rename the variable $x_i : 1 \le i \le n$ appearing in the position $j \in [d]$ (from the left), by a new variable x_{ij} and obtain the polynomial g. We say that g is the set-multilinear polynomial obtained from f. One can view the polynomial g as a commutative polynomial over the variables $x_{ij} : 1 \le i \le n, 1 \le j \le d$. We state a simple fact.

Claim 1. *Let $f(x_1, \ldots, x_n) \in \mathbb{F}\langle X \rangle$ be any noncommutative polynomial of degree d. For $1 \le i \le n$, replace the variable x_i appearing in the position $1 \le j \le d$ by a new variable x_{ij}. Let the new polynomial be $g(x_{11}, \ldots, x_{1d}, \ldots, x_{n1}, \ldots, x_{nd})$. Then $f = 0$ if and only if $g = 0$.*

Proof. The proof follows simply from the observation that the monomials in f and g are in one-one correspondence. □

4 A deterministic PIT for +-regular circuits

In this section we consider noncommutative +-*regular* circuits defined below. These circuits can compute polynomials of exponential degree and a double-exponential number of monomials. However, exploiting their structure we can give a white-box deterministic polynomial time identity test for +-regular circuits that proves Theorem 2.

Definition 2. *A noncommutative circuit C, computing a polynomial in $\mathbb{F}\langle X \rangle$ where $X = \{x_1, x_2, \ldots, x_n\}$, is* +-regular *if it satisfies the following properties:*

- *the circuit is homogeneous.*
- *The + gates in the circuit are partitioned into layers such that if g_1 and g_2 are + gates in a layer then there is no directed path in the circuit between g_1 and g_2.*
- *The output gate is a + gate in a separate layer.*
- *all + gates in a layer are of the same syntactic degree.*
- *every input-to-output path in the circuit goes through exactly one + gate in each layer.*

A simple case of +-regular circuits are homogeneous $\Sigma\Pi^*\Sigma$ circuits which are defined as follows.

Definition 3. *A noncommutative arithmetic circuit C is called a* homogeneous $\Sigma\Pi^*\Sigma$ *circuit if it satisfies following properties:*

- *The output gate is a Σ gate.*
- *All inputs to the output gate are Π gates of the same syntactic degree.*
- *In the circuit, every input to output path goes through a Σ gate (which computes a homogeneous linear form $\sum_{i=1}^{n} \alpha_{ij} x_i$ in the input variables $x_1, x_2 \ldots, x_n$) followed by one or more Π gates and ends at the output Σ gate.*

Likewise, we can define $\Pi^*\Sigma$ circuits.

Remark 1. *We note that, in the commutative setting, regular formulas are considered by Kayal et al. [KSS14]. However, their model of regular formulas is restricted than our model of +-regular circuits.*

The following theorem is crucial to our PIT for +-regular circuits.

Theorem 4. *Let $T(z_1, z_2, \dots, z_s)$ be a noncommutative homogeneous degree-d polynomial over a field $\mathbb{F}$ in noncommuting variables $z_1, z_2, \dots, z_s$. Let $R_1, R_2, \dots, R_s$ be noncommutative homogeneous degree d' polynomials in variables $x_1, x_2, \dots, x_n$ over $\mathbb{F}$ such that $\{R_1, R_2, \dots, R_k\}$ is a maximal linearly independent subset of $\{R_1, R_2, \dots, R_s\}$ over $\mathbb{F}$, where*

$$R_j = \sum_{i=1}^{k} \alpha_{ji} R_i, \quad k+1 \le j \le s, \quad \alpha_{ji} \in \mathbb{F}.$$

For fresh noncommuting variables $y_1, y_2, \dots, y_k$ define linear forms

$$\ell_j = \sum_{i=1}^{k} \alpha_{ji} y_i, \quad k+1 \le j \le s.$$

Then $T(R_1, R_2, \dots, R_s) \equiv 0$ if and only if $T(y_1, y_2, \dots, y_k, \ell_{k+1}, \dots, \ell_s) \equiv 0$.

Proof. The reverse implication is immediate. For, suppose $T(y_1, y_2, \dots, y_k, \ell_{k+1}, \dots, \ell_s) \equiv 0$. Then, by substituting R_i for $y_i, 1 \le i \le k$ we obtain $T(R_1, R_2, \dots, R_s) \equiv 0$.

We now show the forward implication. Suppose $T(R_1, R_2, \dots, R_s) \equiv 0$. As $R_1, R_2, \dots, R_k$ are linearly independent over $\mathbb{F}$ we can find degree-d' monomials $m_1, m_2, \dots, m_k$ such that the $k \times k$ matrix B of their coefficients is of full rank. More precisely, if β_{ji} is the coefficient of m_i in R_j then the matrix

$$B = (\beta_{ji})_{1 \le j, i \le k}$$

is full rank.

Define polynomials

$$R'_j = \sum_{i=1}^{k} \beta_{ji} m_i, 1 \le j \le k \tag{1}$$

$$R'_j = \sum_{i=1}^{k} \alpha_{ji} R'_i, k+1 \le j \le s. \tag{2}$$

Notice that $T(R_1, R_2, \dots, R_s) \equiv 0$ implies $T(R'_1, R'_2, \dots, R'_s) \equiv 0$. This is because every nonzero monomial occurring in $T(R'_1, R'_2, \dots, R'_s)$ precisely consists of all monomials from the set $\{m_1, m_2, \dots, m_k\}^d$ occurring in $T(R_1, R_2, \dots, R_s)$ (with the same coefficient).

Replacing m_i by variable $y_i, 1 \le i \le k$ transforms each R'_j to linear forms

$$\ell'_j = \sum_{i=1}^{k} \beta_{ji} y_i, \quad \text{for } 1 \le j \le k,$$

and

$$\ell'_j = \sum_{i=1}^{k} \alpha_{ji} \sum_{q=1}^{k} \beta_{iq} y_q, \ \text{for } k+1 \le j \le s.$$

Note that the coefficient of any monomial $y_{i_1}y_{i_2}\dots y_{i_d}$ in $T(\ell'_1,\ell'_2,\dots,\ell'_k,\ell'_{k+1},\dots,\ell'_s)$ is same as the coefficient of the corresponding monomial $m_{i_1}m_{i_2}\dots m_{i_d}$ in $T(R'_1,R'_2,\dots,R'_s)$ which is zero. Hence $T(\ell'_1,\ell'_2,\dots,\ell'_k,\ell'_{k+1},\dots,\ell'_s)\equiv 0$. Now, since B is invertible, we can apply the linear map B^{-1} to each of the d positions in the polynomial $T(\ell'_1,\ell'_2,\dots,\ell'_k,\ell'_{k+1},\dots,\ell'_s)$ and obtain $T(y_1,y_2,\dots,y_k,\ell_{k+1},\dots,\ell_s)$, which must be identically zero by Proposition 1. This completes the proof. □

Now, suppose C is a $+$-regular circuit of size s of syntactic degree D computing a polynomial in $\mathbb{F}\langle X\rangle$, where $X=\{x_1,x_2,\dots,x_n\}$. Suppose there are d layers of $+$-gates in C, where we number the $+$-gate layers from bottom upward. Thus, the $+$-gates in layer 1 compute homogeneous linear forms in X. Let $g_1,g_2,\dots,g_m$ be the inputs to the layer 2 $+$-gates. In other words, $g_1,g_2,\dots,g_m$ are the output of the $\times$ gates just below the layer 2 $+$-gates. Let C' be the circuit obtained from C by deleting all gates below $g_1,g_2,\dots,g_m$, and replacing $g_1,g_2,\dots,g_m$ by input variables $y_1,y_2,\dots,y_m$, respectively. Let $T(y_1,y_2,\dots,y_m)$ be the homogeneous degree D' polynomial computed by C'. In the circuit C suppose $P_1,P_2,\dots,P_m$ are the polynomials computed by the gates $g_1,g_2,\dots,g_m$, respectively. As C is homogeneous, each P_i is homogeneous of syntactic degree D/D' (which means either P_i is identically zero or homogeneous degree $D''=D/D'$).

Notice that we can apply Theorem 4 to the polynomials T and $P_1,P_2,\dots,P_m$, and immediately obtain the following.

Lemma 1. *Suppose, without loss of generality, that $P_1,P_2\dots,P_t$ is a maximal $\mathbb{F}$-linearly independent subset of $P_1,P_2,\dots,P_m$, and*

$$P_j=\sum_{i=1}^{t}\alpha_{ji}P_i,\quad t+1\le j\le m.$$

Then $T(P_1,P_2,\dots,P_m)\equiv 0$ if and only if $T(y_1,y_2,\dots,y_t,\sum_{i=1}^t\alpha_{t+1i}y_i,\dots,\sum_{i=1}^t\alpha_{mi}y_i)\equiv 0$.

I.e. the circuit C is identically zero if and only if the circuit $C'(y_1,y_2,\dots,y_t,\sum_{i=1}^t\alpha_{t+1i}y_i,\dots,\sum_{i=1}^t\alpha_{mi}y_i)\equiv 0$.

Clearly, Lemma 1 will yield a deterministic polynomial-time identity test for regular circuits, if we can solve the following problem in deterministic polynomial time:

Given a list of noncommutative polynomials $P_1,P_2,\dots,P_m\in\mathbb{F}\langle X\rangle$, where each P_i is given by a $\Pi^*\Sigma$ circuit, find a maximal linearly independent subset A of the polynomials $P_i, 1\le i\le m$ and express the others as linear combinations of the P_i in A.

The PIT for $+$-regular circuits would follow because we can repeat the same argument as above with C'. Finally, we will be left with verifying if the sum of linear forms (in at most s variables, say $z_i, 1\le i\le s$) vanishes.

4.1 Linear independence testing of $\Pi^*\Sigma$ circuits

In this subsection we solve the above mentioned linear independence testing problem. Namely, we prove the following theorem.

Theorem 5. *Given as input $\Pi^*\Sigma$ circuits computing noncommutative polynomials $P_1,P_2,\dots,P_m\in\mathbb{F}\langle X\rangle$, there is a deterministic polynomial-time algorithm that will find a maximal linearly independent subset A of the polynomials $P_i, 1\le i\le m$, and also express the others as $\mathbb{F}$-linear combinations of the P_i in A.*

Proof. Let $L_1, L_2, \ldots, L_t$ be the set of all linear forms (in variables $x_1, x_2, \ldots, x_n$) defined by the bottom Σ layers of the given $\Pi^*\Sigma$ circuits computing polynomials $P_i, 1 \le i \le m$.

Without loss of generality, let $L_1, L_2, \ldots, L_r$ be a maximal set of linear forms among $L_1, L_2, \ldots, L_t$ that are not scalar multiples of each other. Thus, for each $L_i, i > r$, there is some $L_j, j \le r$ such that L_i is a scalar multiple of L_j. Therefore, we can express each P_i as a product of linear forms from $L_1, \ldots, L_r$, upto a scalar multiple:

$$P_i = \alpha_i L_{i1} L_{i2} \ldots L_{iD}, \quad 1 \le i \le m$$

Corresponding to the linear forms $L_1, L_2, \ldots, L_r$ define an alphabet $\{a_1, a_2, \ldots, a_r\}$ of r letters, where a_i stands for $L_i, 1 \le i \le r$.

Let s be the bound on the sizes of the given $\Pi^*\Sigma$ circuits computing polynomials $P_i, 1 \le i \le m$.

For each i, we can transform the $\Pi^*\Sigma$ circuit computing P_i into a multiplicative circuit C_i of size s computing a word w_i of length D in $\{a_1, a_2, \ldots, a_r\}^D$ as follows: replace linear form L_j in the $\Pi^*\Sigma$ circuit by letter a_k if L_j is a scalar multiple of L_k.

The following claim is immediate.

Claim 2. *Polynomials P_i and P_j are scalar multiples of each other if and only if $w_i = w_j$.*

At this point we recall the following results which are implicit in [Loh15, Pla94, MSU97] about words over a finite alphabet, where the words are given as input by multiplicative circuits (where multiplication is concatenation of words).

- There is a deterministic polynomial time algorithm that takes as input two multiplicative circuits C_i and C_j over a finite alphabet and tests if the words computed by them are identical. If not the algorithm returns the leftmost index k where the two words differ.

- Given a word w by a multiplicative circuit C over some finite alphabet, the following tasks can be done in deterministic polynomial time: computing the length $|w|$ of w, given index k computing the k^{th} letter $w[k]$, circuits C' and C'' that compute the prefix $w[1 \ldots k]$ and $w[k+1 \ldots |w|]$ determined by any given position k, circuit $C_{k,k'}$ for the subword $w[k \ldots k']$ for given positions k and k'. In particular, this implies that the circuit $C_{k,k'}$ is of size polynomial in the sizes of C, k and k'. The parameters k, k' are given in binary.

Thus, given C_i and C_j corresponding to polynomials P_i and P_j, we can find if P_i and P_j are scalar multiples of each other in deterministic polynomial time.

Without loss of generality, let $P_1, P_2, \ldots, P_\ell$ be the polynomials that are *not* scalar multiples of each other. Our aim is to determine a maximal linearly independent subset A of these polynomials, and express each of the remaining polynomials as a linear combination of polynomials in A.

Our algorithm will require a rank bound due to Saxena and Seshadri [SS13]. We recall their result first. Consider a $\Sigma\Pi\Sigma$ arithmetic circuit C', where the top Σ gate has fanin k, all Π gates are of fanin D, and each Π gate computes a product $Q_i, 1 \le i \le k$ of homogeneous $\mathbb{F}$-linear forms in commuting variables $y_1, y_2, \ldots, y_n$. Circuit C' is said to be *simple* if the $gcd(Q_1, Q_2, \ldots, Q_k) = 1$. Circuit C' is said to be *minimal* if for any proper subset $S \subset [k]$ the sum $\sum_{i \in S} Q_i \neq 0$.

If the polynomial computed by a simple and minimal circuit C' is identically zero then it is shown in [SS13] that the rank of the set of all $\mathbb{F}$-linear forms occurring at the bottom Σ layer of the circuit is bounded by $O(k^2 \log D)$.

In order to apply this rank bound in our setting, we make the polynomials $P_i, 1 \le i \le \ell$ set-multilinear in variables $\{x_{im} \mid 1 \le i \le n, 1 \le m \le D\}$ as follows: corresponding to each linear form $L_j, 1 \le j \le r$ we define linear forms $L'_{jm}, 1 \le m \le D$, where L'_{jm} is obtained from L_j by replacing variable x_i with variable x_{im}, for $1 \le i \le n$ and $1 \le m \le D$. Likewise, we obtain the set-multilinear polynomial $\hat{P}_i$ from P_i by replacing the m^{th} linear form, say L_j, with L'_{jm}, for $1 \le m \le D$.[2] The following claim is immediate.

Claim 3. *A linear form L' divides the gcd of a subset S of the polynomials $\hat{P}_i, 1 \le i \le \ell$, if and only if $L' = L'_{jm}$ for some j and m, and L_j occurs in the m^{th} position of each product $P_i \in S$.*

The next claim includes the main step of the algorithm.

Claim 4. *For $i \le \ell$, we can test in deterministic polynomial time if P_i can be expressed as an $\mathbb{F}$-linear combination of $P_1, P_2, \ldots, P_{i-1}$.*

Proof of Claim. Suppose P_i is expressible as an $\mathbb{F}$-linear combination of $P_1, P_2, \ldots, P_{i-1}$. Let $S \subseteq [i-1]$ be a minimal subset such that we can write

$$P_i = \sum_{j \in S} \gamma_j P_j, \quad \gamma_j \neq 0 \quad \text{for all } j.$$

Now, consider the set-multilinear circuit C' defined by the sum of products

$$\hat{P}_i - \sum_{j \in S} \gamma_j \hat{P}_j.$$

By minimality of subset S, circuit C' is minimal. Suppose for some $j \in S$, P_i and P_j disagree on ρ positions. I.e. for ρ positions m, the linear forms occurring in the m^{th} position in P_i and P_j are different. Let the gcd of the polynomials in the set $\{\hat{P}_j \mid j \in S\} \cup \{\hat{P}_i\}$ be P, and let $\deg(P) = \delta$. By the previous claim it follows that

$$\delta \le D - \rho.$$

Define polynomials $Q_i = \hat{P}_i / P$ and $Q_j = \hat{P}_j / P, j \in S$. Notice that each Q_i is a product of $D - \delta$ linear forms. Furthermore, $\hat{P}_i - \sum_{j \in S} \gamma_j \hat{P}_j = P(Q_i - \sum_{j \in S} \gamma_j Q_j)$. Consider the simple and minimal circuit C'' defined by the sum

$$Q_i - \sum_{j \in S} \gamma_j Q_j.$$

Clearly, C' is zero iff C'' is zero. Since C'' is a set-multilinear circuit, the rank of the set of all $\mathbb{F}$-linear forms is at least $D - \delta$. If $C'' \equiv 0$ then by the [SS13] rank bound we have $\rho \le D - \delta \le O(\ell^2 \log(D - \delta))$. Hence, it follows from the inequality $\log_2 x \le x^{1/2}$ that $\rho \le c \cdot \ell^4$, for some constant $c > 0$. Thus, for each $j \in S$, P_i and P_j can disagree on at most $c \cdot \ell^4$ positions.

Therefore, the candidate polynomials $\hat{P}_j, j \le i-1$ in the linear combination for expressing $\hat{P}_i$ are from only those P_j that disagree with P_i in at most $c \cdot \ell^4$ positions. Using the algorithms from [Loh15, Pla94, MSU97] stated above, we can use the multiplicative circuits C_i and C_j and determine if there are at most $c \cdot \ell^4$ positions where the corresponding words differ. We can also compute the at most $c \cdot \ell^4$ many indices where the words differ. Let $S' \subseteq [i-1]$ be the set of all such indices j. Our goal is to efficiently determine if $\hat{P}_i$ is an $\mathbb{F}$-linear combination of the $\hat{P}_j, j \in S'$.

[2] The conversion to the set-multilinear polynomial is only for the sake of analysis and not for the actual algorithm.

Let $T \subset [D]$ be the set of all positions where P_i differs from some $P_j, j \in S'$. Then $|T| \leq c \cdot \ell^5$, and the polynomial P_i and all $P_j, j \in S'$ have identical linear forms in the remaining $[D] \setminus T$ positions. Using the claim 1, it is easy to see that for determining linear dependence, we can drop the linear forms occurring in the positions in $[D] \setminus T$. Thus, we can replace P_i and each $P_j, j \in S'$ with polynomials P'_i and $P'_j, j \in S'$ obtained by retaining only those linear forms occurring in positions in T. [3] We can determine these linear forms for each P_i from the multiplicative circuit C_i in deterministic polynomial time using the results in [Loh15, Pla94].

Clearly each $P'_j, j \in S'$ as well as P'_i is computable by a $\Sigma\Pi\Sigma$ noncommutative circuit of size at most $O(n\ell^5)$. In particular, these polynomials are all computable by $\mathrm{poly}(\ell, n)$ size noncommutative algebraic branching programs (noncommutative ABP). Now, we will apply the main idea from the Raz-Shpilka deterministic polynomial identity test [RS05] to determine if P'_i is a linear combination of the $P'_j, j \in S'$.

We explain concisely how to adapt the Raz-Shpilka algorithm. Let B_i and $B_j, j \in S'$ be the ABPs computing P'_i and $P'_j, j \in S'$, respectively. Following [RS05] we process all the ABPs simultaneously, layer by layer. At the q^{th} layer, we maintain a list of degree-q monomials $m_{1q}, m_{2q}, \ldots, m_{pq}$, along with their coefficient matrix $C(q)$: The j^{th} columns of this matrix gives the vector of coefficients of the monomials $m_{1q}, m_{2q}, \ldots, m_{pq}$ in the polynomial computed in the j^{th} in layer q. Furthermore, for any other degree q monomial m, the coefficient vector of its coefficients at the nodes in layer q is a linear combination of the rows of $C(q)$. Given this data for the q^{th} layer, it is shown in [RS05] how to efficiently compute the monomials and coefficient matrix for layer $q+1$. Continuing thus, when we reach the last layer containing the output gates of B_i and $B_j, j \in S'$, we will have monomials $m_1, m_2, \ldots, m_{\ell'}$ and corresponding $\ell' \times \ell$ coefficient matrix C which has complete information about all linear dependencies between the polynomials P'_i and $P'_j, j \in S'$. In particular, $P'_i = \sum_{j \in S'} \beta_j P'_j$ if and only if $C_1 = \sum_{j \in S'} \beta_j C_j$, where C_1 is the column of coefficients in P'_i and C_j are the columns corresponding to the $P'_j, j \in S'$, which can be determined efficiently using Gaussian elimination. This completes the proof of this claim. □

To conclude the overall proof we note that the above claim can be applied to determine the leftmost maximal linearly independent subset A of the input polynomials $P_1, \ldots, P_m$ and also express the others as linear combinations of polynomials in A. □

5 Black-box randomized PIT for homogeneous $\Sigma\Pi^*\Sigma$

As shown in the previous section, we can test if a given homogeneous $\Sigma\Pi^*\Sigma$ circuit (white-box) is identically zero in deterministic polynomial time (as $\Sigma\Pi^*\Sigma$ circuits are $+$-regular).

However, suppose we have only black-box access to a $\Sigma\Pi^*\Sigma$ circuit C computing a polynomial in $\mathbb{F}\langle X \rangle$. I.e. we can evaluate C on square matrices M_i substituted for $x_i, 1 \leq i \leq n$, where the cost of an evaluation is the dimension of the M_i. Then it is not clear how to apply the observations of the previous section. Specifically, C may compute a nonzero exponential degree noncommutative polynomial, but it is not clear if we can test that by evaluating C on matrices of polynomial dimension. Also, the black-box PIT result of [AMR16] cannot be applied here since C can compute polynomials of double-exponential sparsity.

Nevertheless, we show in this section that if C is an s-sum $P_1 + P_2 + \cdots + P_s$ of D-products of linear forms in variables X. I.e.

$$P_i = L_{i1} L_{i2} \ldots L_{iD},$$

[3] Notice that using Claim 1, $P_i = \sum_{j \in S'} \gamma_j P_j \Leftrightarrow \hat{P}_i = \sum_{j \in S'} \gamma_j \hat{P}_j \Leftrightarrow Q_i = \sum_{j \in S'} \gamma_j Q_j \Leftrightarrow P'_i = \sum_{j \in S'} \gamma_j P'_j$.

where D is exponentially large then we can do black-box PIT for C by evaluating it on random $O(s)\times O(s)$ matrices with entries from $\mathbb{F}$ or a suitably large extension of $\mathbb{F}$. It also clearly follows from our argument that we do not need the top + gate to be homogeneous. We only need the polynomials P_i to be product of homogeneous linear forms. But for notational simplicity we continue writing each P_i as a product of D linear forms. The proof of this claim is based on the notion of projected polynomials defined below which also shows that the homogeneous parts of different degrees can not participate in cancellation of terms.

5.1 Projected Polynomials

Definition 4. *Let $P \in \mathbb{F}\langle X\rangle$ be a homogeneous degree-D polynomial. For an index set $I \subseteq [D]$ the* I-projection *of polynomial P is the polynomial P_I which is defined by letting all variables occurring in positions indexed by the set I as noncommuting. In all other positions we make the variables commuting, by renaming x_i by the commuting variable z_i for $1 \le i \le n$. Thus, the I-projected polynomial P_I is in $\mathbb{F}[Z]\langle X\rangle$, and the (noncommutative) degree of P_I is just I.*

Lemma 2. *Let $P_1, P_2, \ldots, P_s \in \mathbb{F}\langle X\rangle$ each be a product of D homogeneous linear forms*

$$P_i = L_{i,1}L_{i,2}\ldots L_{i,D},$$

where $\{L_{i,j} : 1 \le i \le s, 1 \le j \le D\}$ are linear forms in $\mathbb{F}\langle X\rangle$. Then there exists a subset $I \subseteq [D]$ of size at most $s-1$ such that for any nonzero scalars $\beta_1, \beta_2, \ldots, \beta_s \in \mathbb{F}\setminus\{0\}$ we have

$$\sum_{i=1}^{s} \beta_i P_i = 0 \text{ iff } \sum_{i=1}^{s} \beta_i P_{i,I} = 0,$$

where $P_{i,I}$ is the I-projection of the polynomial P_i.

Proof. The proof is by induction on s. The lemma clearly holds for $s = 1$. By induction hypothesis we assume that an index set of size at most $s-2$ exists for a set of at most $s-1$ polynomials, each of which is a product of D homogeneous linear forms. The forward implication is obvious, because making variables commuting can only facilitate cancellations. We prove the reverse implication.

Suppose that $\sum_{i=1}^{s} \beta_i P_i \neq 0$ for nonzero $\beta_i, 1 \le i \le s$. Let $j_0 \in [D]$ be the least index such that $\text{rank}\{L_{1,j_0}, \ldots, L_{s,j_0}\} > 1$. If no such index exists then the P_i are all scalar multiples of each other in which case $\sum_{i=1}^{s} \beta_i P_i$ is just αP_1 which is zero if and only if $\alpha P_{1,I}$ is zero, and the implication clearly holds.

We can assume, by renumbering the polynomials that $\{L_{1,j_0}, \ldots, L_{t,j_0}\}$ is a maximal linearly independent set in $\{L_{1,j_0}, \ldots, L_{s,j_0}\}$, where $t > 1$.

Then,

$$P_i = c_i P L_{i,j_0} L_{i,j_0+1} \ldots L_{i,D} : 1 \le i \le t$$

$$P_i = c_i P\big(\sum_{k=1}^{t} \gamma_k^{(i)} L_{k,j_0}\big) L_{i,j_0+1} \ldots L_{i,D} : t+1 \le i \le s,$$

where $\{c_i \in \mathbb{F} : 1 \le i \le s\}$, $\{\gamma_k^{(i)} \in \mathbb{F} : 1 \le k \le t, t+1 \le i \le D\}$, and $P \in \mathbb{F}\langle X\rangle$ is a product of homogeneous linear forms (or a scalar). For $1 \le i \le s$, let

$$P_i' = c_i \prod_{j=j_0+1}^{D} L_{i,j}.$$

We can then write

$$\sum_{i=1}^{s}\beta_i P_i = P\big(\sum_{i=1}^{t}\beta_i L_{i,j_0}P'_i\big) + P\big(\sum_{i=t+1}^{s}\beta_i L_{i,j_0}P'_i\big).$$

Note that $P\big(\sum_{i=t+1}^{s}\beta_i L_{i,j_0}P'_i\big) = P\big(\sum_{i=t+1}^{s}\beta_i\big(\sum_{k=1}^{t}\gamma_k^{(i)}L_{k,j_0}\big)P'_i\big)$. Now by rearranging terms, we get the following.

$$\sum_{i=1}^{s}\beta_i P_i = P\big(\sum_{k=1}^{t}L_{k,j_0}P''_k\big)$$

where $P''_k = \beta_k P'_k + \beta_{t+1}\gamma_k^{(t+1)}P'_{t+1} + \ldots + \beta_s\gamma_k^{(s)}P'_s$ for $1 \le k \le t$.

Now, $L_{k,j_0}, 1 \le k \le t$ are linearly independent. Applying Proposition 1, consider any invertible linear map A_{j_0} applied to position j_0 of the polynomial $\sum_{i=1}^{t}\beta_i P_i$ which maps $A_{j_0} : L_{k,j_0} \mapsto x_k, 1 \le k \le t$. Then we have

$$A_{j_0}(\sum_{i=1}^{s}\beta_i P_i) = P\big(\sum_{k=1}^{t}x_k P''_k\big),$$

and $A_{j_0}(\sum_{i=1}^{t}\beta_i P_i) \neq 0$. Thus, not all $P''_k, 1 \le k \le t$ are zero. Assume that $P''_1 \neq 0$. Note that P''_1 is sum of at most $s-1$ polynomials, each of which is a product of homogeneous linear forms. Hence, by induction hypothesis, there is an index set $I' \subseteq \{j_0+1,\ldots,D\}$ of size at most $s-2$ such that

$$P''_{1,I'} = \big(\beta_1 P'_{1,I'} + \beta_{t+1}\gamma_1^{(t+1)}P'_{t+1,I'} + \ldots + \beta_s\gamma_1^{(s)}P'_{s,I'}\big) \neq 0^4.$$

Let $I = I' \cup \{j_0\}$. Now consider the polynomial $\sum_{i=1}^{s}\beta_i P_{i,I}$, which we want to prove to be nonzero. Instead, we prove that $A_{j_0}\big(\sum_{i=1}^{s}\beta_i P_{i,I}\big)$ is nonzero. Notice that

$$A_{j_0}\big(\sum_{i=1}^{s}\beta_i P_{i,I}\big) = \hat{P}\big(\sum_{k=1}^{t}x_k P''_{k,I'}\big),$$

where $\hat{P}$ is the commutative polynomial obtained by replacing x_i by z_i in P. Since $\hat{P}$ is a product of linear forms it remains nonzero. Furthermore, the sum can be zero if and only if each $P''_{k,I'}$ is zero. However, $P''_{1,I'}$ is nonzero. This completes the proof. □

5.2 The black-box identity test

We now describe a *black-box* randomized polynomial time identity testing algorithm for depth three regular circuits. Let $C = \sum_{i=1}^{s} R_i$ be a polynomial in $\mathbb{F}\langle X\rangle$ given as black-box, where each R_i is a product of D homogeneous linear forms. By Lemma 2 there is a set $I \subseteq [D]$ of size at most $s-1$ such that $C = \sum_{i=1}^{s} R_i = 0$ if and only if $\tilde{C} = \sum_{i=1}^{s} R_{i,I} = 0$. Similar to the result in [AMR16], we will use a small size nondeterministic automaton to guess this subset I of locations, and substitute suitable commuting variables at all locations in $[D] \setminus I$. It will turn out that the transition matrices for each variable x_i corresponding to this automaton will give us the desired black-box substitution.

Let $|I| = k \le s-1$. Consider the following nondeterministic finite automaton A whose transition diagram we depict for $x_i : 1 \le i \le n$ in Figure 1. For locations in $[D] \setminus I$, the automaton uses the

[4] If any $\gamma_1^{(j)}$ is zero, we just work with a smaller sum.

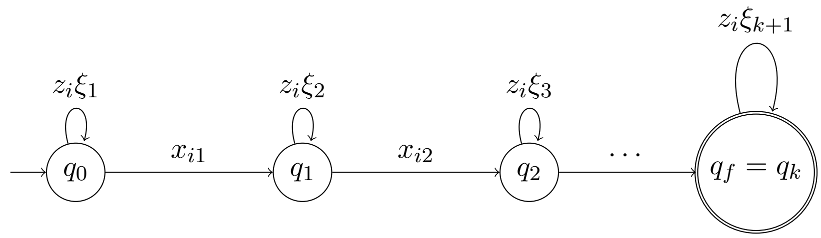

Figure 1: The transition diagram for the variable $x_i : 1 \leq i \leq n$

block variables $Z = \{z_i : 1 \leq i \leq n\}$, $\xi = \{\xi_i : 1 \leq i \leq k+1\}$ which are commuting variables. For each index location $j \in I$ the automaton substitutes x_i by $x_{ij}, 1 \leq i \leq n$, where the index variables $Z' = \{x_{ij} : 1 \leq i \leq n, 1 \leq j \leq k\}$ are also commuting variables.

Remark 2. *Notice that in Lemma 2, the variables occurring in positions in I were left as noncommuting. However, the automaton we construct replaces x_i in position $j \in I$ by commuting variable x_{ij}. This transformation for homogeneous polynomials is known to preserves identities by Claim 1.*

Let

$$\forall i \in [s] : R_i = L_{i,1} \dots L_{i,D}.$$

Let M_{x_i} be the matrix corresponding to variable $x_i, 1 \leq i \leq n$. When we do this matrix substitution to variables in R_i, the $(0,k)^{th}$ entry of the resulting matrix M_{R_i} is

$$\widehat{R}_i = \sum_{(j_1,j_2,\dots,j_k)\in[D]^k} \prod_{j=1}^{j_1-1} L_{i,j}(Z){\xi_1}^{j_1-1} L_{i,j_1}(Z') \prod_{j=j_1+1}^{j_2-1} L_{i,j}(Z){\xi_2}^{j_2-j_1-1} L_{i,j_2}(Z') \dots\dots$$

For each $i \in [s]$, the polynomial $\widehat{R}_i \in \mathbb{F}[Z, \xi, Z']$. The $(0,k)^{th}$ entry of the resulting matrix M_C is

$$\sum_{i=1}^{s} \widehat{R}_i = \sum_{J\in[D]^k} P_J \xi_J,$$

where $\xi_J = \xi_1^{j_1-1}\xi_2^{j_1-j_2-1}\dots\xi_k^{D-j_k}$ and $P_J = \sum_{i=1}^{s} P_{i,J}$.

By Lemma 2, we know that $P_I = \sum_{i=1}^{s} P_{i,I} \neq 0$. Thus, $\sum_{i=1}^{s} \widehat{R}_i$ is nonzero, as the monomials sets for different P_J are disjoint (ensured by the terms ξ_J). The degree of $\sum_{i=1}^{s} \widehat{R}_i$ is D. So if $|\mathbb{F}|$ is more than D, it can not evaluate to zero on $\mathbb{F}$. This completes the proof of Theorem 3.

Now the randomized identity testing algorithm follows by simply random substitution for variables in the commutative polynomial computed at the $(0,k)^{th}$ entry of the resulting matrix M_C. This completes the proof of Corollary 1.

6 Conclusion

The main open problem is to find a randomized polynomial time identity test for general noncommutative circuits (in the white-box model). Our result for +-regular circuits is a first step towards that. Finding an efficient randomized black-box identity testing algorithm for +-regular circuits is also an interesting problem. For homogeneous $\Sigma\Pi^*\Sigma$ circuits, we have obtained such a randomized black-box identity test.

References

[AGKS15] Manindra Agrawal, Rohit Gurjar, Arpita Korwar, and Nitin Saxena, *Hitting-sets for ROABP and sum of set-multilinear circuits*, SIAM J. Comput. **44** (2015), no. 3, 669–697.

[AL50] Avraham Shimshon Amitsur and Jacob Levitzki, *Minimal identities for algebras*, Proceedings of the American Mathematical Society **1** (1950), no. 4, 449–463.

[AM08] Vikraman Arvind and Partha Mukhopadhyay, *Derandomizing the isolation lemma and lower bounds for circuit size*, Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques, 11th International Workshop, APPROX 2008, and 12th International Workshop, RANDOM 2008, Boston, MA, USA, August 25-27, 2008. Proceedings, 2008, pp. 276–289.

[AMR16] Vikraman Arvind, Partha Mukhopadhyay, and S. Raja, *Randomized Polynomial Time Identity Testing for Noncommutative Circuits*, ECCC Report no. 89, 2016.

[AMS08] Vikraman Arvind, Partha Mukhopadhyay, and Srikanth Srinivasan, *New results on noncommutative and commutative polynomial identity testing*, Proceedings of the 23rd Annual IEEE Conference on Computational Complexity, CCC 2008, 23-26 June 2008, College Park, Maryland, USA, 2008, pp. 268–279.

[BW05] Andrej Bogdanov and Hoeteck Wee, *More on noncommutative polynomial identity testing*, 20th Annual IEEE Conference on Computational Complexity (CCC 2005), 11-15 June 2005, San Jose, CA, USA, 2005, pp. 92–99.

[DL78] Richard A. DeMillo and Richard J. Lipton, *A probabilistic remark on algebraic program testing*, Inf. Process. Lett. **7** (1978), no. 4, 193–195.

[FS13] Michael A. Forbes and Amir Shpilka, *Quasipolynomial-time identity testing of noncommutative and read-once oblivious algebraic branching programs*, 54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA, 2013, pp. 243–252.

[Hya77] Laurent Hyafil, *The power of commutativity*, 18th Annual Symposium on Foundations of Computer Science, Providence, Rhode Island, USA, 31 October - 1 November 1977, 1977, pp. 171–174.

[KSS14] Neeraj Kayal, Chandan Saha, and Ramprasad Saptharishi, *A Super-polynomial Lower Bound for Regular Arithmetic Formulas*, Proceedings of the 46th Annual ACM Symposium on Theory of Computing, STOC, 2014, pp. 146–153.

[Loh15] Markus Lohrey, *Equality Testing of Compressed Strings*, WORDS, 2015, pp. 14–26.

[MSU97] Kurt Mehlhorn, R. Sundar, and Christian Uhrig, *Maintaining Dynamic Sequences under Equality Tests in Polylogarithmic Time*, Algorithmica **17**, 1997, no. 2, 183–198.

[Pla94] Wojciech Plandowski, *Testing Equivalence of Morphisms on Context-Free Languages*, Algorithms - ESA '94, Second Annual European Symposium, Utrecht, The Netherlands, September 26-28, 1994, pp. 460–470.

[Nis91] Noam Nisan, *Lower bounds for non-commutative computation (extended abstract)*, STOC, 1991, pp. 410–418.

[RS05] Ran Raz and Amir Shpilka, *Deterministic polynomial identity testing in non-commutative models*, Computational Complexity **14** (2005), no. 1, 1–19.

[SS13] Nitin Saxena and C. Seshadhri, *From Sylvester-Gallai configurations to rank bounds: Improved blackbox identity test for depth-3 circuits*, Journal of the ACM, **60**(2013), no 5, 1–34.

[Sch80] J. T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, J. ACM **27** (1980), no. 4, 701–717.

[Zip79] Richard Zippel, *Probabilistic algorithms for sparse polynomials*, Symbolic and Algebraic Computation, EUROSAM '79, An International Symposium on Symbolic and Algebraic Computation, Marseille, France, June 1979, Proceedings, 1979, pp. 216–226.

[WACT16] WACT 2016, *Some Accessible Open Problems*, `https://www.cs.tau.ac.il/~shpilka/wact2016/concreteOpenProblems/openprobs.pdf`, Workshop in Algebraic Complexity Theory, Tel Aviv, February 7–12, 2016.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de